Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Protecting the Privacy of Customers of	)	WC Docket No. 16-106
Broadband and Other Telecommunications	)	
Services	)	

COMMENTS OF CINCINNATI BELL TELEPHONE COMPANY LLC

Douglas E. Hart
441 Vine Street, Suite 4192
Cincinnati, Ohio 45202
(513) 621-6709
(513) 621-6981
dhart@douglasehart.com

Attorney for Cincinnati Bell
Telephone Company LLC

May 27, 2016

I. INTRODUCTION AND SUMMARY

In its Notice of Proposed Rulemaking, ("NPRM"), released April 1, 2016 in this docket, the Commission invited comment on a variety of topics related to the privacy of information regarding broadband Internet access service ("BIAS") customers. Cincinnati Bell Telephone Company LLC ("Cincinnati Bell or CBT") is a mid-sized incumbent local exchange company operating in parts of Ohio, Kentucky and Indiana and provides BIAS over both fiber and copper network facilities. CBT offers comments from its perspective on several of the issues raised in the NPRM.

CBT is also a member of USTelecom and the ITTA and joins in their separate comments, being filed in this docket. The Commission's proposed rules unfairly single out ISPs and treat them in far more restrictive fashion than the rest of the Internet industry. On March 1, 2016, a broad group of Internet industry participants, including USTelecom, submitted a detailed proposal for a broadband privacy framework. CBT urges the Commission to adopt that proposal as its approach to privacy protection for BIAS rather than the one put forth in the NPRM. The proposal urged the Commission to draw from the FTC's approach, which controlled before the Commission's reclassification of BIAS as a Title II service. If the Commission adopts privacy rules as proposed in the NPRM, it should avoid creating a new regime and instead rely upon frameworks that are already in place, such as that used by the FTC with respect to the same industry.

A summary of CBT's separate comments is as follows:

- Regulation of privacy practices of BIAS providers should await resolution of the Commission's Title II jurisdiction over ISPs
- Privacy regulation should not be expanded beyond CPNI as specified in § 222 of the Telecommunications Act

- Any regulation of personally identifiable information beyond CPNI should be specific and narrowly crafted and only target situations that are truly harmful to consumers
- The Commission should not micromanage the customer authentication process, but only establish principals for privacy protection and leave BIAS providers to design systems that accomplish them
- The Commission should not prohibit deep packet inspection and other advanced services that would be of value to consumers
- ISPs should not be subject to an opt-in consent regime but should be allowed to continue using the opt-out process
- The Commission should not impose onerous breach notification and reporting rules
- The Commission should not require detailed supervision of third parties but allow BIAS providers to rely upon contractual promises.

II. COMMENTS

A. The Commission Should Not Create New Broadband Customer Privacy Rules

The NPRM relies upon the Commission's Open Internet Order and its decision to reclassify BIAS as a Title II communications service. CBT will not address the issue of legal authorization for the Commission to classify BIAS as a Title II service herein, except to note that the Open Internet Order is currently subject to legal challenge. If it does not survive that challenge, there is no basis for the Commission to create privacy practices for BIAS.

It is only recently that the Commission has asserted jurisdiction over BIAS by declaring it a Title II service within its statutory jurisdiction. Many parties have questioned the Commission's ability to reclassify BIAS as a telecommunications service or to assert jurisdiction, and CBT does not waive any argument that BIAS is beyond the Commission's regulatory reach. Thus, these comments are being submitted conditionally in case the courts affirm the Commission's assertion of jurisdiction. In any event, CBT would urge the

Commission to refrain from creating new BIAS privacy rules until the jurisdictional question is resolved.

B. The Commission Should Not Create a Definition of CPI to include CPNI and PII.

The Customer Proprietary Network Information ("CPNI") rules designed for legacy telephone services were based upon the statutory grant of authority in 47 U.S.C. § 222 and, specifically, the definition of CPNI in § 222(h). The Commission would expand § 222 far beyond the protection of CPNI to include Personally Identifiable Information ("PII"). Section 222(c) and (h) were designed to address specific concerns about telephone call records and bill information.

If the Commission has authority to and chooses to apply CPNI principles to ISPs, it should follow the same approach that has been followed to date and not vastly expand the coverage of CPNI to include PII. Proposed Rules 64.2003(h) and 64.7000(f) would define Customer Proprietary Information ("CPI") as including both CPNI and PII.

For ISPs that were telecommunications service providers prior to the reclassification of BIAS as telecommunications, the customer base for traditional telecommunications services and that for BIAS are largely the same, so systems are already in place than can be adapted to cover CPNI for both customer groups. However, the Commission's new definitional approach to CPI to also include PII could require significant and expensive systems changes. Essentially, the Commission's PII regime should mirror the existing FTC definitions, breach parameters and response requirements, and guidance for protecting sensitive data.

While Cincinnati Bell does not feel these significant and expensive systems changes are justified on their own merit, given the present uncertainty over the Commission's jurisdiction to regulate BIAS it would be wasteful to require ISPs to abide by a whole new set of rules when the

jurisdictional underpinnings of the rules could fail. The Commission should, at a minimum, wait until its jurisdiction over BIAS is confirmed before embarking on such a regulatory endeavor.

C. Any Definition Of Customer Proprietary Information Should Remain Narrow and Be Specific.

Preferably, the Commission would define CPNI in a way that addresses concerns about BIAS customers specifically and narrowly, in keeping with the principles of §§ 222(c) and (h). Many of the proposed CPNI elements must be disclosed for BIAS to function.

First, the Commission proposes that CPNI in the BIAS context should include such things as geo-location, media access control (MAC) addresses, and source and destination IP addresses. But these items should not be considered CPNI because this information is necessarily sent onto the open Internet in order to make the service work.

Geo-location can be derived from ISP addresses, which are an inherent part of Internet traffic and are necessarily disclosed. Unlike switched voice traffic, where a dedicated path was created between calling and called party, the Internet uses addresses embedded in the packet traffic itself in order to route information to and from its intended destination. The Commission recognizes that there is an exception to disclosure when it is necessary to provide service and the IP address is perhaps the most fundamental thing that is necessary to provide service. An ISP cannot be expected to protect the confidentiality of CPE originated addressing information in providing service. Cincinnati Bell would urge that any privacy restriction on disclosing such address information be limited to the simultaneous disclosures of the *combination* of a MAC or IP address with truly sensitive personally identifiable customer information that is not itself a component of the Internet traffic.

Next, the proposed definition of PII is extremely broad and vague. Proposed Rule 64.7000(i) would include as PII any information that is linked or "linkable" to an individual.

The term "linkable" is overly broad and vague, such that the Commission's rules would not restrict the universe of causalities by which some information might be linkable to an individual only to things that are within the control of the ISP.

There needs to be a clearly delineated definition of CPI and of what is a breach. It is debatable that any information that can be linked to an individual merits confidential protection, so the definition of PII should be narrowed to include those items that could reasonably be expected to harm consumers if disclosed by a BIAS provider.

The individual elements identified as PII in the NPRM should be limited to the already effective and durable definitions from the FTC, and should not be defined as PII independently – only when used in combination with the customer's identity is such information subject to misuse that could result in harm to the consumer.

For example, a customer's IP address must be used by an ISP in order to direct traffic to the correct location and cannot be kept confidential if the service is to work. Furthermore, any time customers identify themselves on a website for any purpose, they are disclosing the combination of their personally identifiable information and are using the ISP to transmit that information. It should only be in the context of an ISP itself using combinations of information for unauthorized purposes, or when an ISP's internal systems are breached in order to access such information in combination, that an ISP should have any responsibility for the disclosure.

Internet traffic often contains personal information intentionally sent by the customer, including names, addresses, social security numbers, credit card numbers, account numbers, etc. Once data packets go onto the open Internet, an ISP has no control over their security. The ISP's responsibilities should be limited to protection of data that the ISP maintains in its own systems.

Lastly, Proposed Rule 64.2000(e) would define "customer" to also include applicants for BIAS. The Commission should clarify that this term is only intended to include potential customers who actually submit PII to an ISP as part of an application for BIAS. For example, prospective customers may visit an ISP's commercial website to learn about the services offered. In that case, the ISP would be acting in the same capacity as any other Internet content provider, not as a BIAS provider, and it should not be required to treat the visitor as a BIAS customer. Prospective customers should not be treated as "applicants" if they do not request service from the ISP nor should any data that is collected during the course of their visit be considered CPI. This is more reason to defer to the FTC regime for privacy CPI type information as that would put BIAS and Edge providers on the same footing.

D. The Commission Should Keep Customer Authentication Processes Reasonable

Proposed Rule 64.7005 would essentially make an ISP the insurer of security for all customer PII. Responsibility for a security breach should not be a strict liability analysis, but should be based upon fault and whether a BIAS provider acts reasonably. Because cybersecurity defense methods and the attack vectors deployed against them evolve at an ever-increasing rate, the Commission should not attempt to codify behavior. Rather, it should future-proof its rules by encouraging BIAS providers to keep pace with rapid developments in the industry (*i.e.*, act reasonably).

Part (4) of the rule would require "robust customer authentication procedures" to grant anyone access to CPI. The Commission has sought comment on methods of providing customer authentication. Cincinnati Bell believes the Commission should continue to allow ISPs to rely upon customer provided passwords as the main security gateway. Instead of forcing rigid syntax rules (e.g., requiring certain characters), which may actually provide impostors with information

as to the proper format of a valid password, ISPs should be allowed to offer flexible password strength and security features similar to current banking industry and Governmental agency practices when users set up access to their account information.

Similar to means now being used by taxing authorities to verify the identity of filers, an ISP could ask the customer to verify some unique account information that the ISP can validate. CBT would suggest a knowledge-based approach that would require the customer to verify various pieces of information that only they should know about. If the customer can verify the information, the ISP could text or e-mail the customer an access code that would be used to log in with the user id and password on the account. Users with a secure cookie/token could be allowed in with only a user id and password.

E. The Commission Should Not Prohibit Deep Packet Inspection Nor Secure-By-Design Services

The Commission is contemplating a ban on deep packet inspection for purposes other than network management. (NPRM, ¶ 264.) Deep Packet Inspection and URL filtering are routinely used for managed firewalls and parental controls. The Commission should clarify that these types of uses are considered to be within the definition of "network management" so as to not preclude ISPs from providing these services. Furthermore, this approach would unfairly treat ISPs differently from Edge and website content providers that routinely engage in such practices.

The FTC does not prohibit the use of such practices for marketing purposes, so long as the user discloses its use in its privacy policy. The Commission did not identify any flaws in the FTC framework that required a different approach. The Commission's proposed rule is overly paternalistic and could prevent customers from receiving services or benefits that they would like. It would also inhibit the ability of ISPs, particularly those that offer public WiFi services, from creating innovative new services that rely upon those practices. As such, the Commission's

proposed rules would impede innovation, increase costs to do business, and impair the ability of companies to develop new uses for information that could benefit consumers and provide additional revenue streams. And it would do so in a way that disproportionately impacts small- and mid-size BIAS providers like Cincinnati Bell, who lack the vast resources of their mega-sized competitors to innovate rapidly despite new regulatory complexities.

Last, the Commission proposes a prohibition on offering higher-priced broadband services for heightened privacy protection. The Commission should not prohibit such practices. Heightened security measures do not come without cost. And a prohibition against the secure-by-design products and services that BIAS providers currently offer and continue to develop will impoverish consumers rather than protect them. The Commission should consider cost benefit analysis when setting the basic privacy protection rules, as all service customers will be entitled to that level of protection. Once the basic privacy requirements are established on such a basis, the Commission should not prohibit BIAS providers from offering enhanced levels of security for customers who are willing to pay the extra cost that is necessary to support such services.

F. The Commission Should Not Expand The Use Of Opt-In Consent

The proposed opt-in rules are not tied to the sensitivity of the information being used, but rather to the nature of its use. Consumers are accustomed to having their data used for targeted marketing – the entire business model of the giant content providers is predicated on this practice. It is somewhat absurd to allow an ISP to use CPI to market a different type of BIAS to its customer, but not to allow it to market accessories they might use with the service. And, non-BIAS provider websites and search engines, which gather massive amounts of personal data on customers and non-customers who visit or use their sites, are subject to no regulation as to how they use the data so long as it is consistent with their privacy policies.

The NPRM would change the dynamics of opt-in and opt-out consent to use of CPI. Rule 64.7002(a) presumes customer approval of the use of CPI only for purposes of provisioning service, billing, fraud prevention, for inbound marketing, and support of PSAPs in emergency situations. An ISP may use CPI to market additional BIAS offerings in the same category of service (fixed or mobile BIAS) only if the customer already subscribes to that category of service. An ISP may use opt-out approval for purposes of marketing communications-related services itself (a narrowly defined category),[1] but must obtain affirm opt-in consent from the customer to make any other use of the information. The Commission should not impose opt-in rules for use of CPI on BIAS providers but should instead adopt the FTC approach to privacy.

The FTC does not have specific privacy rules, but instead enforces privacy through enforcement actions against false or deceptive advertising practices if providers violate their stated privacy policies. Privacy policies should remain voluntary, flexible and promote a risk management approach. The reclassification of BIAS as a Title II service removes the FTC's authority over that segment of the Internet industry, but provides no compelling reason to treat providers of BIAS differently than they were treated before reclassification, or differently than the thousands of Internet content providers that consumers continue to access which operate under the FTC regime. The FTC approach of giving an effective privacy policy notice to consumers and the choice to not allow the use of their data is equally effective for BIAS providers as it is for others, and an opt-in regime is unnecessary. In contrast, the NPRM overrides consumer preferences with the Commission's policy choices and would mandate specific practices without any showing of consumer harm.

[1] 47 C.F.R. § 64.2003(k) would define "Information services typically provided by telecommunications carriers" as excluding retail consumer services provided using websites. Presumably this would preclude telecommunications carriers who act as ISPs from using CPI to market their other consumer services or sharing CPI with communications related affiliates who provide retail services through websites.

Many of the practices the NPRM addresses are concerned with marketing practices, not consumer harm. The use of data to produce targeted advertising is not a security or privacy issue and is largely how the Internet works.

ISPs should not be unfairly singled out from engaging in a practice vis-à-vis the rest of an Internet industry that is inarguably beyond the Commission's jurisdiction. Such practices only increase the cost of providing BIAS and harm consumers in the long run. Just as free over the air television is supported by commercial advertising, so is much of the Internet. To require ISPs to play by a different set of rules than everyone else in the Internet ecosystem will only disadvantage ISPs relative to content providers.

Opt-out procedures have been available for use of CPNI in the telephone industry for many years and have worked well. The Internet is a very different space than telephone service and should have less, not more restrictive rules. Consumers expect and want to have valuable offers brought to their attention. Unlike unwanted telemarketing calls, robocalls, spam and the like, Internet marketing is not disruptive.

It is the sensitivity of information that should drive how it is treated, not the nature of the entity that holds the information. Thus, ISPs should not be bound by different and more onerous rules than Edge providers, search engines, or websites that have the same or more access to sensitive customer data. Only unfair or deceptive conduct should be proscribed. The Commission's approach to privacy protection should be as similar as possible to that followed by the FTC, which continues to govern the conduct of non-carrier participants in the Internet.

Telecommunications service providers should be free to adopt privacy policies of their choosing, describing what customer information they collect, how they will use it, and whether and how it will be shared with third parties. So long as the policy is clear and disclosed to customers, and not unfair or deceptive, carriers' conduct should then be judged by their

adherence to their stated privacy policies. Most consumers have a choice of service providers and privacy policies themselves can become a part of the competitive choice calculus.

G. The Commission Should Not Impose Onerous Breach Notification Rules

The breach notification requirements should be changed to be more practical and consistent with current CPNI practice and defer to the already robust breach notification regime of the FTC when it comes to PII. Proposed 47 C.F.R. § 64.2011(a)(1) would require a customer notification within 10 days after the discovery of a breach. Part (a)(2) requires that the notice contain specific details about the breach that may not be available in the brief time frame allowed – the time should not begin until the service provider has forensic information sufficient to identify the scope of the breach. It takes time to investigate whether a breach has actually occurred and to determine the scope of the impact. Companies should not be required to notify consumers before they have all the facts, which could lead to customer confusion. The Commission should not require carriers to give customers premature notices inconsistent with those policies, nor to provide notices when critical information about the suspected data breach is not available.

Unlike the existing § 222 CPNI rules, the proposed new rules do not require intent and are not limited to situations of real customer harm. Proposed Rules 64.2003(d) and 64.7000(b) would define a "breach of security" to include any situation where person accesses CPNI without authorization or exceeding authorization. This definition is vague and overbroad. What determines if a person accessing an account "exceeds" their authorization? If a customer has authorized someone to access their account, the ISP will not know the extent of authority the customer gave that person. The ISP should not be responsible for a third party exceeding the authorization that the customer provided – the ISP should only be responsible when a third party accesses an account with no authorization. And, in cases where the account access was by an

ISP employee, but was inadvertent or there was not external disclosure of CPI, there should be no obligation to report that circumstance as a "breach" as the customer suffered no harm or potential harm.

Proposed Rule 64.7005(a)(5) would require a notification to the customer any time there is a change in account information (not just the password). The Commission should consider the IT costs necessary to implement such a system and balance those against the anticipated benefits to the consumer. The rule would also require a BIAS provider to notify the customer of any attempt to access CPI. This could require an ISP to notify a customer every time the customer accesses his or her own CPI, or if the customer makes a mistake in logging in, or if a third party accidentally attempts to log into the wrong account but does not actually log in. This rule is overkill. It could require an expensive overhaul of BIAS providers' systems in order to detect and report such activity and will likely result in numerous false alarms to customers. All when there is no actual or potential harm to any consumer.

H. The Commission Should Not Impose Onerous Supervisory Rules

The Commission should not impose unrealistic logging requirements, particularly on smaller providers. The size and capability of the ISP matter in determining what is reasonable. While it may be reasonable to require an ISP to maintain a log of access to customer accounts, it may be unreasonable to require routine reviews of such logs. Only in case of a breach or claimed breach should the actual review of logs be mandated.

The proposed program to police compliance by third parties is too broad. Service providers should be permitted to rely upon contractual assurances from their contractors that privacy considerations will be honored. Often, the purpose of contracting with a third-party is because the service provider does not have the internal resources to manage the function that is being outsourced. If the service provider is charged with micromanaging the operations of the

third party, the benefit of outsourcing could be lost. Service Providers should not be privacy police for their contractors, but should only have to do appropriate due diligence with some ongoing review of technical controls at a high level. ISPs cannot be expected to oversee and be responsible for every minute action of their contractors and the employees of their contractors, ad infinitum. Contractors should be permitted to represent, warrant, and covenant that they are in compliance and will comply without the service provider having to conduct extensive auditing. In such a situation, it is the contractor that should assume primary responsibility for compliance with Commission rules and be accountable directly to the Commission (which is the FTC framework today).

The Commission should not create a Consumer Privacy Dashboard. It will cause ISPs to incur great expense out of line with the benefit. Such a requirement could involve vast IT expenditures with little customer benefit. The cost of creating the Dashboard would be particularly onerous on smaller providers and might lead to higher prices or force these providers to divert resources that could be used to enhance their cybersecurity or expand broadband deployment. Similarly, the Commission should not specify the content and frequency of training for employees, nor should there be mandatory training of contractors and affiliates – principals should be allowed to rely upon the contractor to perform that task.

The Commission seeks comment on whether it should establish a "safe harbor" with respect to risk management assessments. While a safe harbor is sometimes nice to have, if the Commission creates safe harbors, it should offer realistic scenarios that carriers can reasonably comply with without undue burden or expense. The safe harbor should pass a risk/reward analysis such that the burden of compliance is not excessive. Further, the Commission should

not treat a "safe harbor" as the only path to compliance – too often, a safe harbor becomes a minimum standard and not just one possible alternative means of compliance.

III. CONCLUSION

The Commission should not adopt privacy rules for ISPs at this time. There is too much legal uncertainly regarding the Commission's jurisdiction over BIAS and no demonstrated need for immediate action. Even assuming the Commission does have jurisdiction over BIAS, the rules should not go as far as proposed in the NPRM. The FTC has already promulgated a framework of rules with which all BIAS providers must comply today. CBT urges the Commission to relax the proposed rules as suggested in these comments and in the comments filed by USTelecom and the ITTA.

Respectfully submitted,

Douglas E. Hart
441 Vine Street, Suite 4192
Cincinnati, Ohio 45202
(513) 621-6709
(513) 621-6981
dhart@douglasehart.com

Attorney for Cincinnati Bell
Telephone Company LLC